FOURTH ASSIGNMENT

Group number: *Acme-30*

Student Names and Numbers

Emanuele Santo Iaia	1924549
Simone Giordano	1772347

Initial Brainstorming

For this assignment, we are doing a reuse of what we did in the first assignment.

Rsyslog Setup

To provide a functioning log server to store the log files created by the hosts of the network, we worked on the log server host in the server network. First of all, we added the following in the /etc/rsyslog.conf file:

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%HOSTNAME%.log"
*.* ?RemoteLogs
& ~
```

Thanks to this, whenever the log server receives a log input from an external host, it creates a .log file with the name of the source in the /var/log directory.

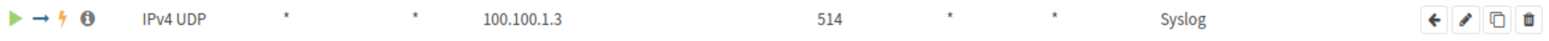
To make it possible to receive the log file into the standard UDP port, we simply removed the “#” comment to the “#Provides UDP Syslog reception”.

Regarding the host configuration, we also modified the rsyslog.conf file, in order to send all the log also to the server address thanks to the following line:

```
*.* @100.100.1.3:514
```

Where the @ means that the log messages are sent via UDP protocol together with the IP address of the log server and the defined port in the rsyslog.conf of the log server.

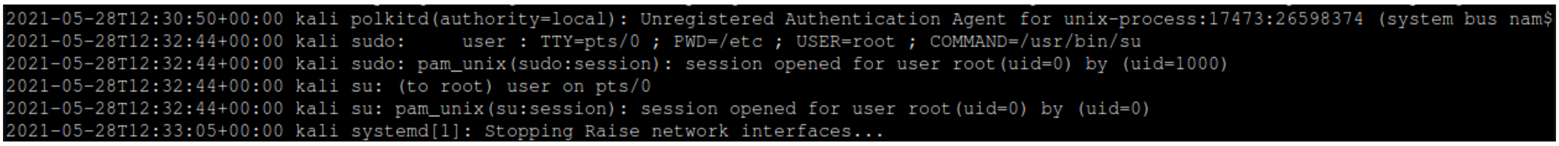
We also added the firewall rule to handle the correct sending of the syslog rules:



IPv4 UDP	*	*	100.100.1.3	514	*	*	Syslog

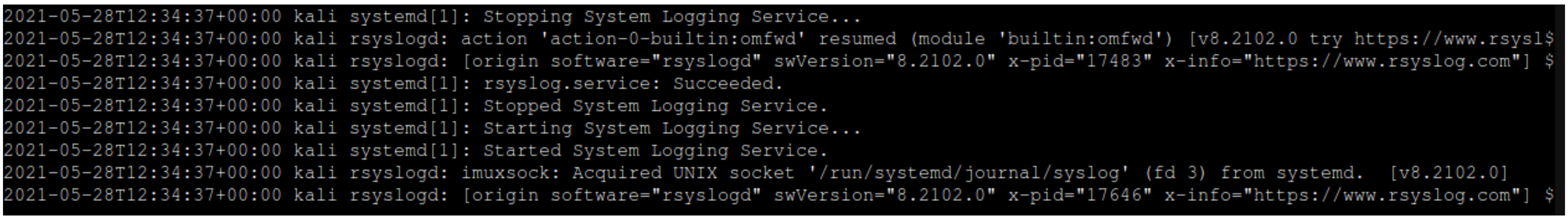
Performed tests

To test the correctness of the logging, we moved on the log server, in particular in the folder relevant to the kali machine in the clients network: “*/var/log/kali/kali.log*”.
Firstly we did a screenshot of the current state of the machine that was the following:



```
2021-05-28T12:30:50+00:00 kali polkitd(authority=local): Unregistered Authentication Agent for unix-process:17473:26598374 (system bus nam$
2021-05-28T12:32:44+00:00 kali sudo:     user : TTY=pts/0 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/su
2021-05-28T12:32:44+00:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
2021-05-28T12:32:44+00:00 kali su: (to root) user on pts/0
2021-05-28T12:32:44+00:00 kali su: pam_unix(su:session): session opened for user root(uid=0) by (uid=0)
2021-05-28T12:33:05+00:00 kali systemd[1]: Stopping Raise network interfaces...
```

Then we performed a rsyslog restart on the kali machine with the following command: ”/etc/init.d/rsyslog restart” and we checked that this action was corrected sent and stored on the log file related to the kali machine (the same as before) as we can see below:



```
2021-05-28T12:34:37+00:00 kali systemd[1]: Stopping System Logging Service...
2021-05-28T12:34:37+00:00 kali rsyslogd: action 'action-0-builtin:omfwd' resumed (module 'builtin:omfwd') [v8.2102.0 try https://www.rsysl$
2021-05-28T12:34:37+00:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="17483" x-info="https://www.rsyslog.com"] $
2021-05-28T12:34:37+00:00 kali systemd[1]: rsyslog.service: Succeeded.
2021-05-28T12:34:37+00:00 kali systemd[1]: Stopped System Logging Service.
2021-05-28T12:34:37+00:00 kali systemd[1]: Starting System Logging Service...
2021-05-28T12:34:37+00:00 kali systemd[1]: Started System Logging Service.
2021-05-28T12:34:37+00:00 kali rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2102.0]
2021-05-28T12:34:37+00:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="17646" x-info="https://www.rsyslog.com"] $
```

Final remark

The rsyslog configuration is one the easier setup to configure a system logging in the network, this method could be really powerful to handle large networks and to detect errors in the systems.